REMARKS

In response to the Office Action of November 28, 2003, Applicants respectfully request reconsideration. To further the prosecution of this application, each of the rejections set forth in the Office Action is addressed below. Claims 1, 3, 4, 5, and 8 are amended herein and claims 31-33 are newly added. The application is believed to be in condition for allowance.

Claim Objections

At page 13, paragraph 8, the Office Action objected to claim 5, asserting that the phrase "generating use a hash" is unclear. Applicants respectfully disagree, as claim 5 previously recited that the steps of generating recited in claim 4 use a hash function. Nevertheless, to further the prosecution of this application, Applicants have amended claim 5 to recite that the act of generating the first file identifier further comprises generating the first file identifier using a first hash function and the act of generating the second file identifier further comprises generating the first file identifier using a second hash function. This amendment is made solely for the purpose of clarification and does not alter the scope of the claim.

Rejections Under 35 U.S.C. §112

The Office Action rejected claims 3 and 7 under 35 U.S.C. §112, second paragraph, asserting that, "[t]he terms 'third file identifier' and 'fourth file identifier' are vague. The prior claims did not include a first and a second file identifier that pertains to the existence of the third and fourth file identifier." (Page 2, paragraph 5 of Office Action).

With regard to the rejection of claim 3, Applicants have amended the claim to recite "first file identifier" instead of "third file identifier" and "second file identifier" instead of "fourth file identifier." These amendments are made solely for the purpose of clarification and do not alter the scope of the claim. Applicants respectfully request the rejection of claim 3 under 35 U.S.C. §112, second paragraph be withdrawn.

With regard to the rejection of claim 7, Applicants note that claim 7 depends from claim 4, which recites both a "first file identifier" and a "second file identifier." Therefore, Applicants believe the use of the terms "third file identifier" and "fourth file identifier" in claim 7 does not implicate the clarity concern raised in the Office Action. Accordingly, Applicants respectfully request that the rejection of claim 7 under 35 U.S.C. §112, second paragraph be withdrawn.

Rejections Under 35 U.S.C. §102

The Office Action rejected claims 1-5, 7-10, 13, 14, 18, and 20-30 under 35 U.S.C. §102(e) as purportedly being anticipated by Saito (6,076,077). Applicants respectfully traverse this rejection.

Discussion of Saito (6,076,077)

Saito is directed to a data management system and discloses several embodiments in which copyrighted data is protected using one or more public-private key pairs and/or one or more symmetric keys (*see, e.g.,* Col. 7, lines 49-53; Col. 10, lines 5-9; Col. 12, lines 45-54; Col. 16, line 3 – Col. 18, line 42). These keys are generated independently of the data that they are used to encrypt. Nowhere does Saito disclose that any of the keys used to encrypt data is computed from the content of the data that is encrypted by the key. Additionally, Saito does not disclose that any of these keys is used to uniquely identify and/or retrieve data.

Summary Of Embodiments of Applicants' Invention

An example of one embodiment of Applicants' invention is described below to highlight some distinctions between Applicants' claimed invention and the cited references. Support for the example below may be found in Applicants' specification at page 11, lines 18 – page 16, line 4. It should be appreciated that the description below is merely an example of one of many embodiments that fall within the scope of Applicants' claims and is provided merely for the purpose of highlighting distinctions between Applicants' claims and the cited reference.

One embodiment of the invention is directed to encrypting a binary asset. As shown in Figure 1 below, an intrinsic unique identifier (IUI) is generated from at least a portion of the contents of a binary asset. That is, one input to the process which generates the IUI is all of or a portion of the binary asset. As an example, the process which generates the IUI may be a hash function which hashes all or a portion of the binary asset

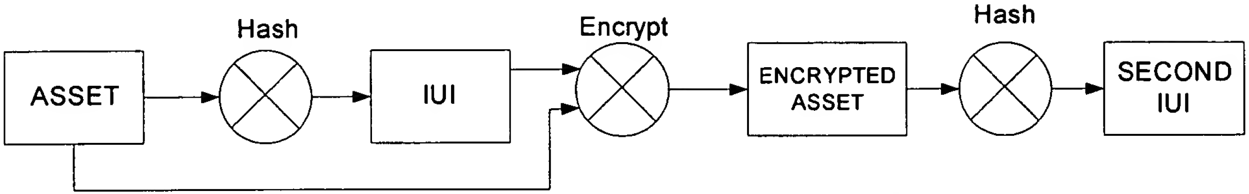

Figure 1

The IUI and the asset then may be provided as inputs to an encryption function, wherein the IUI is used as a key to encrypt the binary asset, as shown above in Figure 1. The output of the encryption function is an encrypted binary asset.

Figure 1 highlights an aspect of the encryption keys used in embodiments of the present invention that clearly distinguishes from the encryption keys used in Saito. In the above-described embodiment of the present invention, a key used to encrypt an asset is generated from all or a portion of the asset. For example, the key may be generated by hashing the asset and then using the result of the hash as the key. **Saito does not disclose or suggest generating a key from all or a portion of data to be encrypted**.

In addition, embodiments of the present invention use an encryption key that not only is based on the content of the asset, but is in fact an intrinsic unique identifier (IUI) for the asset. Saito does not disclose computing a unique identifier for each file or separate piece of data content, let alone using a unique identifier as an encryption key. Instead, Saito discloses using the same key to encrypt many different pieces of data content.

Further, in some embodiments of the present invention, a second IUI may be generated for the encrypted asset from all or a portion of the encrypted asset (e.g., by hashing), as shown above in Figure 1. The second IUI may be used as an identifier to locate the encrypted asset. That is, an entity requesting access to an encrypted asset may provide the second IUI for that asset to identify which encrypted asset is being requested. An example is shown in Figure 2, wherein a requesting entity sends the second IUI to a receiving entity. If the receiving entity has a copy of the encrypted asset from which the second IUI was generated, then the receiving entity may send a copy of the encrypted asset to the requesting entity. By contrast, Saito does not disclose providing an identifier that is computed from a portion of an asset to locate or retrieve the asset.

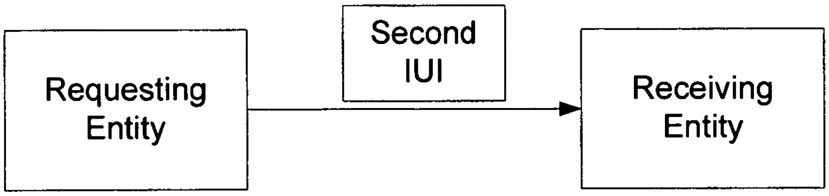

Figure 2

In summary, Saito does not disclose or suggest computing identifiers for data from a portion of that data, nor the encrypting of data based on such an identifier. In embodiments of the present invention identifiers (i.e., IUIs) may be computed from all or a portion of a binary asset. These identifiers may be used, for example, as keys to encrypt/decrypt the binary asset or as identifiers to locate and/or retrieve the binary asset.

The foregoing summary is provided merely to assist the Examiner in appreciating various aspects of the present invention. The summary may not apply to each of the independent claims, and the language of the independent claims may differ in material respects from the summary provided. The Examiner is requested to give a careful consideration to the language of each of the independent claims and to address each on its own merits, without relying on the summary provided above. Applicants do not rely on the summary to distinguish any of the claims of the present invention over the prior art, but rather, rely only upon the arguments provided below.

Claim 1

Claim 1 is directed to a method comprising: generating a first unique identifier for a binary asset, said first unique identifier being computed from at least a portion of the contents of said binary asset and uniquely identifying said binary asset; and encrypting said binary asset using said first unique identifier as a key, said encrypting resulting in an encrypted version of said binary asset.

The Office Action asserts that Saito discloses "a unique identifier that was generated for the file that was computed from at least a portion of the contents and that uniquely identifies the file" at column 7, lines 38-55. (page 3, paragraph 6 of Office Action). The Office Action further asserts that "the Examiner also asserts that the unique identifier can be a key such as a secret or common key or a public key type wherein the key is used to identify the file." (page 4, lines 1-2, of Office Action). Applicants respectfully disagree with these assertions.

The cited section of Saito (column 7, lines 38-55) discloses the use of two public-private key pairs (i.e., Kb1, Kv1 and Kb2, Kv2) and two symmetric secret keys (i.e., Ks1 and Ks2) which are used to manage the distribution of copies of data. Nowhere does Saito disclose that these keys are computed from at least a portion of the contents of a binary asset.

Furthermore, there is no basis for the Examiner's assertion that any key disclosed by Saito serves as a unique identifier for a file. Saito merely discloses that the keys are used to encrypt data content and/or other keys. Nowhere does Saito disclose or suggest that a file may be identified by an encryption key. Indeed, Saito discloses that one key may be used to encrypt multiple different units of data content (*see, e.g.,* Col. 8, lines 4-18 of Saito). If the same key is used to encrypt multiple different files, then that key clearly does not uniquely identify a single file.

Thus, Saito fails to disclose or suggest, *inter alia*, "generating a unique identifier for said binary asset, said unique identifier being computed from at least a portion of the contents of said binary asset and uniquely identifying said binary asset" or "encrypting said binary asset using said first unique identifier as a key, said encrypting resulting in an encrypted version of said binary asset," as recited in claim 1. Accordingly, it is respectfully requested that the rejection of claim 1 under 35 U.S.C. §102(e) be withdrawn.

Claims 2 and 3 depend from claim 1 and are patentable for at least the same reasons. Accordingly, it is respectfully requested that the rejection of claims 2 and 3 be withdrawn.

Claim 4

Claim 4 is directed to a method comprising: generating a first file identifier for a file, said first file identifier being computed from at least a portion of said file and uniquely identifying said file; encrypting said file using said first file identifier as a key, said encrypting producing an encrypted file; generating a second file identifier for said encrypted file, said second file identifier being computed from at least a portion of said encrypted file and uniquely identifying said encrypted file; and providing said first file identifier and said second file identifier for the retrieval of said file, whereby said second file identifier may be used to locate said encrypted file, and said first file identifier may be used to decrypt said encrypted file to produce said file.

As should be clear from the discussion above, Saito fails to disclose or suggest, *inter alia*, "generating a first file identifier for a file, said first file identifier being computed from at least a portion of said file and uniquely identifying said file" and "encrypting said file using said first file identifier as a key." As discussed above, the keys in Saito are not computed from a portion of the content which they encrypt and do not uniquely identify a file. Accordingly, it is respectfully requested that the rejection of claim 4 under 35 U.S.C. §102(e) be withdrawn.

Claims 5-7 depend from claim 4 and are patentable for at least the same reasons. Accordingly it is respectfully requested that the rejections of claims 5-7 be withdrawn.

Claim 8

Claim 8 is directed to a method of uniquely and securely identifying a group of binary assets, each binary asset representing digital information. The method comprises: computing an intrinsic unique identifier (IUI) for each of said binary assets; encrypting each of said binary assets using the IUI of each asset as its key to produce an encrypted version of each of said binary assets; computing an IUI of each of said encrypted versions; creating a file that includes said IUIs of said binary assets and said IUIs of said encrypted versions; computing a key IUI for said file; encrypting said file using said key IUI to produce an encrypted file; and computing a master IUI for said encrypted file, whereby said key IUI and said master IUI uniquely represent said binary assets and may be used to locate said assets.

As should be clear from the discussion above, Saito fails to disclose or suggest, *inter alia*, "computing an intrinsic unique identifier (IUI) for each of said binary assets" and "encrypting each of said binary assets using the IUI of each asset as its key to produce an encrypted version of each of said binary assets," as recited in claim 8. Saito does not disclose computing a unique key to encrypt each asset. Instead, Saito discloses using the same key to encrypt multiple different pieces of data content. Accordingly, it is respectfully requested that the rejection of claim 8 under 35 U.S.C. §102(e) be withdrawn.

Claims 9-12 depend from claim 8 and are patentable for at least the same reasons. Accordingly it is respectfully requested that the rejections of claims 9-12 be withdrawn.

Claim 13

Claim 13 is directed to a descriptor file data structure that reliably identifies a plurality of files. The data structure comprises: a file name for each of said files; meta data for each file indicating attributes of each file; a first intrinsic unique identifier (IUI) for each of said files, each IUI being calculated from the contents of its corresponding file and uniquely identifying its corresponding file; and a second IUI associated with each of said files, each second IUI being calculated from an encrypted version of its associated file, each file being encrypted using its associated first IUI as a key, wherein said second IUIs may be used to locate said encrypted versions of said files, and said first IUIs may be used to decrypt said encrypted versions to obtain the non-encrypted versions of said files.

As should be clear from the discussion above, Saito fails to disclose or suggest, *inter alia*, a data structure that identifies a plurality of files comprising "a first intrinsic unique identifier (IUI) for each of said files, each IUI being calculated from the contents of its corresponding file and uniquely identifying its corresponding file" and "a second IUI associated with each of said files, each second IUI being calculated from an encrypted version of its associated file, each file being encrypted using its associated first IUI as a key," as recited in claim 13. Accordingly, it is respectfully requested that the rejection of claim 13 under 35 U.S.C. §102(e) be withdrawn.

Claim 14 depends from claim 13 and is patentable for at least the same reasons. Accordingly it is respectfully requested that the rejection of claim 14 be withdrawn.

Claim 18

Claim 18 is directed to a method of reliably retrieving a secure file. The method comprises: receiving an intrinsic unique identifier for an encrypted version of said file; retrieving said encrypted version of said file using said IUI of said encrypted versions; receiving an IUI for the non-encrypted version of said file; and decrypting said encrypted version of said file using said IUI of said non-encrypted version as a key to obtain the non-encrypted version of said file, whereby said IUI of said encrypted version and said IUI of said non-encrypted version provide access to the contents of said file.

Saito fails to disclose or suggest, *inter alia*, "decrypting said encrypted version of said file using said IUI of said non-encrypted version as a key to obtain the non-encrypted version of said file" as recited in claim 18. Nowhere does Saito disclose or suggest decrypting an encrypted version of a file using an IUI of the non-encrypted version as a key. The keys disclosed by Saito do not serve as unique identifiers for a file, as these keys may be used to encrypt multiple different files. Accordingly, it is respectfully requested that the rejection of claim 18 under 35 U.S.C. §102(e) be withdrawn.

Claims 19 and 20 depend from claim 18 and are patentable for at least the same reasons. Accordingly, it is respectfully requested the rejections of claims 19 and 20 be withdrawn.

Claim 21

Claim 21 is directed to a method of obtaining a data file that has been securely stored. The method comprises: receiving a master identifier that uniquely identifies an encrypted file; retrieving said encrypted file using said master identifier; receiving a key identifier that uniquely identifies the non-encrypted version of said encrypted file; decrypting said encrypted file using said key identifier to obtain said non-encrypted version, said non-encrypted version including a data file identifier that uniquely identifies a data file and an encrypted version of said data file; retrieving said encrypted version of said data file using said encrypted identifier; and decrypting said encrypted data file using said data file identifier as a decryption key, whereby said non-encrypted version of said data file is obtained.

As should be clear from the discussion above, Saito fails to disclose or suggest, *inter alia*, "receiving a key identifier that uniquely identifies the non-encrypted version of said encrypted file" and "decrypting said encrypted file using said key identifier to obtain said non-encrypted version," as recited in claim 21. In Saito, the keys that are used to decrypt data are not key identifiers that uniquely identify the non-encrypted version of the data. Accordingly, it is respectfully requested that the rejection of claim 21 under 35 U.S.C. §102(e) be withdrawn.

Claims 22-25 depend from claim 21 and are patentable for at least the same reasons. Accordingly, it is respectfully requested that the rejection of claims 22-25 be withdrawn.

Claim 26

Claim 26 is directed to a method of obtaining a data file that has been securely stored. The method comprises: receiving a user identifier that uniquely identifies a non-encrypted first file, said non-encrypted first file including a unique identifier identifying an encrypted version of said data file and a master identifier that uniquely identifies an encrypted version of a descriptor file; retrieving said non-encrypted first file using said user identifier; retrieving said encrypted descriptor file using said master identifier; retrieving said encrypted data file using said unique identifier for said encrypted version of said data file; receiving a key identifier that uniquely identifies the non-encrypted version of said encrypted descriptor file; decrypting said encrypted descriptor fie using said key identifier to obtain said non-encrypted version of said descriptor file, said non-encrypted version including a data file identifier that uniquely identifies said data file; and decrypting said encrypted data file using said data file identifier as a decryption key, whereby said non-encrypted version of said data file is obtained.

As should be clear from the discussion above, Saito fails to disclose or suggest, *inter alia*, "receiving a key identifier that uniquely identifies the non-encrypted version of said encrypted descriptor file" and "decrypting said encrypted descriptor fie using said key identifier to obtain said non-encrypted version of said descriptor file," as recited in claim 26. Accordingly, it is respectfully requested that the rejection of claim 26 under 35 U.S.C. §102(e) be withdrawn.

Claims 27-30 depend from claim 26 and are patentable for at least the same reasons. Accordingly, it is respectfully requested that the rejection of claims 27-30 be withdrawn.

Rejections Under 35 U.S.C. §103

The Office Action rejected claims 6, 11, and 19 under 35 U.S.C. §103(a) as purportedly being obvious over Saito in view of Berkowitz (5,832,479) and claims 12 and 15-17 as being purportedly obvious over Saito in view of Microsoft Computer Dictionary, 5th Edition. Applicants respectfully traverse each of these rejections.

Claims 6, 11, 12, and 19 are dependent claims, and each is patentable for at least the same reasons as the claim from which it depends. Claims 15-17 are discussed below.

Claim 15

Claim 15 is directed to a method of uniquely and securely identifying a group of files. The method comprises: creating a key file that includes a plurality of cryptographic keys, each key being associated with one of said group of files; computing a unique identifier for said key file, said key file identifier being calculated from a portion of the contents of said key file; encrypting said key file using said key file identifier to produce an encrypted key file; computing a unique identifier for said encrypted key file, said encrypted key file identifier be calculated from a portion of the contents of said encrypted key file; creating a flattened file that includes said encrypted key file identifier and unique identifiers for encrypted version of said files, each unique identifier of one of said encrypted files being calculated from the contents of its associated encrypted file, each encrypted file having been encrypted using its associated key to encrypted the plaintext version of the file; and computing a user unique identifier for said flattened file, said user unique identifier be calculated from a portion of the contents of said flattened file, whereby a user provided with said user unique identifier may retrieve said flattened file and said encrypted versions of said files, and when provided with said key file identifier said user may decrypt said encrypted files.

The Office Action asserts that Saito discloses all the limitations of claim 15, except that Saito fails to explicitly teach a flattened file. The Office Action further asserts that the Microsoft Computer Diction discloses a flattened file and that it would have been obvious to use a flattened file in the system of Saito "because it significantly reduces file sized and can be saved in a wider range of formats." (*see* Page 12 of Office Action). Applicants respectfully disagree with these assertions.

1. There Is No Motivation To Combine The References

The Microsoft Computer Dictionary merely provides a definition for the term "flatten." Applicants do not deny that "flattened files" are known in the prior art. However, a mere definition of the term "flatten" would not have motivated one of skill in the art to incorporate flattened files into the data management system disclosed by Saito. Indeed, the Office Action does not even disclose which files in Saito would purportedly be flattened by combining the Saito and the Microsoft Computer Dictionary or how such flattening would be performed.

Because there is no motivation to combine the references, the combination is improper and should be withdrawn.

2. Claim 15 Patentably Distinguishes Over The Combination

Even if one were to combine Saito and the Microsoft Computer Dictionary, Applicants' claims still distinguish over the combination. As should be clear from the discussion above, Saito fails to disclose or suggest, *inter alia*, "computing a unique identifier for said key file, said key file identifier being calculated from a portion of the contents of said key file" and "encrypting said key file using said key file identifier to produce an encrypted key file," as recited in claim 15. Accordingly, it is respectfully requested that the rejection of claim 15 under 35 U.S.C. §103 be withdrawn.

Claims 16 and 17 depend from claim 15 and are patentable for at least the same reasons. Accordingly, it is respectfully requested that the rejection of claims 16 and 17 be withdrawn.

CONCLUSION

In view of the foregoing amendments and remarks, this application should now be in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below to discuss any outstanding issues relating to the allowability of the application.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Respectfully submitted,

Paul R. Carpentier et al., Applicant

By:

Richard F. Giunta, Reg. No. 36,149
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, Massachusetts 02210-2211
Telephone: (617) 720-3500

Docket No. E0295.70188US00
Date: March 1, 2004